UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/882,810	06/14/2001	Shannon J. Chan	MS1-789US	7986

22801 7590 03/17/2006

LEE & HAYES PLLC
421 W RIVERSIDE AVENUE SUITE 500
SPOKANE, WA 99201

EXAMINER	
ARANI, TAGHI T	
ART UNIT	**PAPER NUMBER**
2131	

DATE MAILED: 03/17/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/882,810	CHAN ET AL.	
	Examiner	Art Unit	
	Taghi T. Arani	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *12/16/2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-30* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-30* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Taghi T. Arani
Primary Examiner
AU 2131

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-30 have been examined and are pending.

Response to Amendment

2. This Office action is responsive to Applicant's amendment filed on December 16, 2005.

Applicant's arguments with respect to claims 1-29 have been considered but are moot in view of the new ground (s) of rejection.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 1, 3-4, 6-11, 13, 17-21, 23-25, 27-28 and 30 are rejected under 35 U.S.C. 103(a) as being unpatentable over prior art of record, Spies et al, USP 6,055,314 (hereinafter Spies) and further in view of US patent 6,636,689 to Stebbings.

As per claim 1, Spies teaches a server device including a DVD drive, wherein the server device further includes a key exchange server, and wherein a DVD is accessible to the DVD drive (col., 3, lines 44-50, i.e. video content delivery system includes a video content provider which may or may not be the same as the video merchant and a video encryption device at the video content provider supplies a video data stream in encrypted format on a distribution medium, such as a distribution network or a digital video disk (DVD), col. 5, lines 35-45, where provider computing unit 34 moves cryptographic program keys 42 for

those programs that the video merchant is authorized to sell into a secure key store 40 located at the merchant's facility or accessible by a video merchant computing unit 44. The program keys are conveyed to the secure key store 40 via a secure or unsecure link or physically ported on a floppy diskette, or other means, see also col. 12, lines 49-55, where the video input is implemented either as a network port connected to receive the video data stream from a distribution network or an optical reader for reading the video data stream from a DVD);

a client device coupled to the server device via a network (col. 5, lines 55-col. 6, line 33), the client device including a key exchange client and a decoder (col. 2, lines 32 - 59); and

wherein the key exchange client and the key exchange server communicate with one another to pass one or more keys from the DVD to the key exchange client (col. 6, lines 55-58, i.e. the merchant computing unit 54 downloads the cryptographic key 56 over the distribution network to the purchaser IC card 50) to allow the decoder to decrypt content received, via the network, from the DVD (col. 3, lines 40-45).

While Spies teaches downloading the cryptographic key from the merchant unit (server device) to the client IC card and that the cryptographic keys are ported to the merchant units on a floppy diskette or other means, Spies fails to disclose passing one or more keys from the DVD to the key exchange client, the one or more keys from the DVD also usable to verify authenticity of the DVD drive

However, in an analogous art, Stebbings teaches method and system providing multiple decryption key(s) from the DVD (col. 22, lines 57 through col. 23, line 2) and

authentication key for at least one media and data stored on the media by reading mixed data (audio and video) from a media; detecting at least one authentication key (pit track modulated data, i.e. a key from the DVD to verify the authenticity of the DVD drive); authenticating at least one of the media; and removing pit track modulated data from the mixed data via a decoding operation and outputting at least one of audio, video data (col. 13, 4-12, lines 42 through col. 14, line 4, see also, col. 22, lines 62-through col. 23, line2, Figs. 27-29 and associated texts for network implementation of Stebbings).

Therefore, it would have been obvious to one of ordinary skill in the art to modify Spies' system and method for secure purchase and delivery of video content programs with the teachings of Stebbings's passing one or more keys from the DVD to the key exchange client, the one or more keys from the DVD also usable to verify authenticity of the DVD drive with a motivation to prevent at least one of piracy, unauthorized access and unauthorized copying of the data stored on the media (DVD) (Stebbings , col. 13, lines 47-58).

As per claim 3, Spies teaches the decoder has no knowledge that the DVD drive is included as part of the server device (col. 12, lines 25-30).

As per claim 4, Spies teaches the key exchange server comprises a remote procedure call (RPC) server (col. 6, line 35).

As per claim 6, Spies teaches the network comprises a public network (col. 2, lines 60-63).

As per claim 7, Spies teaches the network comprises a home network (col. 9, line 4).

As per claim 8, Spies teaches the keys are used for DVD movie content. DVD movies are protected by CSS, therefore, this limitation is inherently taught by Spies.

As per claim 9, Spies teaches the decoder is implemented as part of a media content player implemented completely on the client device (col. 9, lines 18-20).

As per claim 10, Spies teaches the decryption of DVD movies. The standard for DVD movie includes using region information in the decryption algorithm. Therefore Spies teaches this limitation.

As per claim 11, Spies teaches pit least one of the keys is specific to a media content player incorporating the decoder, and wherein the server component obtains, based on information received from the client component, the appropriate key for the media content player (col. 12, lines 9-15).

As per claim 13, Spies teaches receiving a request, from a remote client computing device, to obtain one or more keys located on a removable storage medium readable by the server device (col. 5, lines 35-45, where the cryptographic keys are ported to the merchant key store physically on a floppy diskette, or other means, col. 6, lines 34-58, col. 13, lines 24-30, col. 4, lines 35-53), wherein the one or more keys are for decrypting content [on the removable storage medium] (col. 12, lines 25-30); obtaining the one or more keys from the removable storage medium (col. 6, lines 34-58, see also, col. 12, lines 9-11); and communicating the one or more keys to the remote client computing device (col. 12, lines 25-30).

While Spies teaches downloading the cryptographic key from the merchant unit (server device) to the client IC card and that the cryptographic keys are ported to the

merchant units on a floppy diskette or other means, Spies fails to disclose one or more keys for decrypting content on the removable storage medium and for verifying authenticity of the DVD drive.

However, in an analogous art, Stebbings teaches method and system for providing the ability to not only have authentication keys on a track-by-tack basis, but also multiple component keys that need to be combined for validation and for purpose of playing a disc in that an address pointer is used which instructs a player's server to go to the designated disc location containing decryption keys, and read that location (col. 22 line 57 through col. 23, line 2,see also col. 13, lines 4-12, lines 42 through col. 14, line 4, col. 22, lines 62-through col. 23, line2, Figs. 27-29 and associated texts for network implementation of Stebbings).

Therefore, it would have been obvious to one of ordinary skill in the art to modify Spies' system and method for secure purchase and delivery of video content programs with the teachings of Stebbings's one or more keys for decrypting content on the removable storage medium and for verifying authenticity of the DVD drive with a motivation to prevent at least one of piracy, unauthorized access and unauthorized copying of the data stored on the DVD (Stebbings, col. 13, lines 47-58).

As per claim 19, Spies teaches receiving, from a media player executing on the computing device, a request to perform at least part of a key exchange process with a disc drive in order to decode media content on a disc accessible to the disc drive (col. 13, line 24-30, see also col. 5, lines 35-45, where the cryptographic keys are physically ported on a floppy diskette (disc), or other means to the merchant unit); and

communicating, with a remote server (merchant unit) at which the disc drive (the diskette or other means) is located, to obtain one or more keys (col. 6, lines 34-58, where the merchant computing unit downloads the cryptographic keys over the distribution network to the purchaser IC card) from the disc (diskette, or other means) that can be used at the computing device to decode the particular media content (col. 12, lines 8-30).

While Spies teaches downloading the cryptographic key from the merchant unit (server device) to the client IC card and that the cryptographic keys are ported to the merchant units on a floppy diskette or other means, Spies fails to disclose the one or more keys from the disc also usable to verify authenticity of the disc drive.

However, in an analogous art, Stebbings teaches method and system providing multiple decryption key(s) from the DVD (col. 22, lines 57 through col. 23, line 2) and authentication key for at least one media and data stored on the media by reading mixed data (audio and video) from a media; detecting at least one authentication key (pit track modulated data, i.e. a key from the DVD to verify the authenticity of the DVD drive); authenticating at least one of the media; and removing pit track modulated data from the mixed data via a decoding operation and outputting at least one of audio, video data (col. 13, 4-12, lines 42 through col. 14, line 4, see also, col. 22, lines 62-through col. 23, line2, Figs. 27-29 and associated texts for network implementation of Stebbings).

Therefore, it would have been obvious to one of ordinary skill in the art to modify Spies' system and method for secure purchase and delivery of video content programs with the teachings of Stebbings's passing one or more keys from the also usable to verify authenticity of the disc drive with a motivation to prevent at least one of piracy, unauthorized

access and unauthorized copying of the data stored on the disc (Stebbings, col. 13, lines 47-58).

As per claim 24, Spies teaches a server component configured to receive Content Scrambling System (CSS) key requests from a client component on a client device via a network col., 12, lines 8-53;

While Spies teaches downloading the cryptographic key from the merchant unit (server device) to the client IC card and that the cryptographic keys are ported to the merchant units on a floppy diskette or other means, Spies fails to disclose wherein the server component, in conjunction with the client component, operates as an intermediary between a DVD player on the client device and a DVD drive on the server device.

However, in an analogous art, Stebbings teaches method and system wherein an intermediary (col. 26, line 42 through col. 27, line10, i.e. an authentication module at the ISP) providing authentication key or keys between the DVD player on the client device and a DVD drive on the server side (i.e. efile containing electronic video or audio into which authentication key is reproduced).

Therefore, it would have been obvious to one of ordinary skill in the art to modify Spies' system and method for secure purchase and delivery of video content programs with the teachings of Stebbings's authentication module with a motivation to prevent at least one of piracy, unauthorized access and unauthorized copying of the data stored on the disc (Stebbings, col. 13, lines 47-58).

As per claim 27, Spies teaches a key exchange server component configured to interact with a key exchange client component on a remote client system in order to

exchange Content Scrambling System (CSS) keys between [a DVD drive of] the system and the key exchange client component; and wherein the CSS keys are exchanged for use by a DVD content player implemented completely at the remote client system (col. 12, lines 8-53).

While Spies teaches downloading the cryptographic key from the merchant unit (server device) to the client IC card and that the cryptographic keys are ported to the merchant units on a floppy diskette or other means, Spies fails to disclose that the key exchange server configured to interact between a DVD drive of the system and the key exchange client.

However, in an analogous art, Stebbings teaches method and system wherein an intermediary (col. 26, line 42 through col. 27, line10, i.e. an authentication module at the ISP) providing authentication key or keys between the DVD player on the client device and a DVD drive on the server side (i.e. efile containing electronic video or audio into which authentication key is reproduced).

Therefore, it would have been obvious to one of ordinary skill in the art to modify Spies' system and method for secure purchase and delivery of video content programs with the teachings of Stebbings's authentication module with a motivation to prevent at least one of piracy, unauthorized access and unauthorized copying of the data stored on the disc (Stebbings, col. 13, lines 47-58).

As per claim 30, Spies teaches a system comprising.

a server device including a DVD drive, wherein the server device further includes a key exchange server, and wherein a DVD is accessible to the DVD

drive (col., 3, lines 44-50, i.e. video content delivery system includes a video content provider which may or may not be the same as the video merchant and a video encryption device at the video content provider supplies a video data stream in encrypted format on a distribution medium, such as a distribution network or a digital video disk (DVD), col. 5, lines 35-45, where provider computing unit 34 moves cryptographic program keys 42 for those programs that the video merchant is authorized to sell into a secure key store 40 located at the merchant's facility or accessible by a video merchant computing unit 44. The program keys are conveyed to the secure key store 40 via a secure or unsecure link or physically ported on a floppy diskette, or other means, see also col. 12, lines 49-55, where the video input is implemented either as a network port connected to receive the video data stream from a distribution network or an optical reader for reading the video data stream from a DVD);

a client device coupled to the server device via a network (col. 5, lines 55-col. 6, line 33), the client device including a key exchange client and a decoder (col. 2, lines 32 - 59); and

wherein the key exchange client and the key exchange server communicate with one another keys [from the DVD] to the key exchange client, at least one of the keys to allow the decoder to decrypt content received, via the network, [from the DVD], and another of the keys is specific to a media content player incorporating the decoder, and wherein the server component obtains, based on information (col. 13, lines 35-52, Fig. 8 and associated text).

Spies fail to disclose that key exchange server exchange keys from the DVD and that the decoder decrypts content received from the DVD. That is, the recited DVD contains both keys and encrypted content accessible by the DVD drive.

However, in an analogous art, Stebbings teaches method and system providing multiple decryption key(s) from the DVD (col. 22, lines 57 through col. 23, line 2) and authentication key for at least one media and data stored on the media by reading mixed data (audio and video) from media; detecting at least one authentication key (pit track modulated data, i.e. a key from the DVD to verify the authenticity of the DVD drive); authenticating at least one of the media; and removing pit track modulated data from the mixed data via a decoding operation and outputting at least one of audio, video data (col. 13, 4-12, lines 42 through col. 14, line 4, see also, col. 22, lines 62-through col. 23, line2, Figs. 27-29 and associated texts for network implementation of Stebbings).

Therefore, it would have been obvious to one of ordinary skill in the art to modify Spies' system and method for secure purchase and delivery of video content programs with the teachings of Stebbings's passing keys from the DVD_to verify authenticity of the DVD drive and to decrypt the encrypted content on the DVD with a motivation to prevent at least one of piracy, unauthorized access and unauthorized copying of the data stored on the disc (Stebbings, col. 13, lines 47-58).

As per claims 17, 25, and 28, Spies teaches the key exchange server comprises a remote procedure call (RPC) server (col. 6, line 35).

As per claims 17, 25, and 28, Spies teaches the key exchange server comprises a remote procedure call (RPC) server (col. 6, line 35).

As per claims 18 and 23, Spies teaches one or more computer-readable memories containing a computer program that is executable by a processor to perform the method recited in claim 13 (col. 12, line 8).

As per claim 20, Spies teaches the disc comprises an optical disc (col. 12, line 53).

As per claim 21, Spies as modified teaches the decoder has no knowledge that the DVD drive is included as part of the server device (col. 12, lines 25-30).

4. Claims 2, 12, 14, 15, 16, 26, and 29 are rejected under 35 U.S.C. 103(a) as being unpatentable over Spies and Stebbings as applied to claims 1, 13, 24 and 27 above, and further in view of PowerFile C20 FAQs, hereinafter PowerFile (prior art of record).

As per claims 2, 15, 26, and 29, Spies as modified teaches that the user can download videos from DVD but is silent in explicitly discloses the DVD come from a DVD changer. Powerfile teaches a device whereby remote users can download DVD content from a DVD changer over a network (page 2). In view of this it would have been obvious to one of ordinary skill in the art at the time or the invention to employ the teachings of PowerFile within the system of Spies because DVD can be safely stored in DVD changers and are accessible to authorized user.

As per claims 12, 14, and 16, Spies as modified is silent in disclosing that the server and client of a video on demand system are executing on a Windows operating system. Powerfile's DVD on demand system are executing on Windows operation systems. In view of this it would have been obvious to one of ordinary skill in the art at the time of the invention to employ the teachings of Powerfile within the system of Spies because PC are operated by Windows' systems.

5. **Claims 5 and 22** are rejected under 35 U.S.C. 103(a) as being unpatentable over Spies and Stebbings as applied to claims 1 and 19, and further in view of a description of DirectShow (twww.compressionworks.com).

As per claims 5 and 22, Spies as modified teaches that the client uses a media application to view the downloaded content. Spies is silent in disclosing that the media application is DirectShow. DirectShow is a user application, which accepts streamed Video such as MPEG. MPEG is the data compression method used on DVD video. In view of this it would have been obvious to one of ordinary skill in the art at the time of the invention to employ the teachings of DirectShow within the system Spies because Spies teaching streaming DVD content and DirectShow is a capable user application which performs this functionality.

Note: Examiner has pointed out particular references contained in the prior arts of record in the body of this action for the convenience of the applicant. Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claim, other passages and figures may apply as well. Applicant should consider the entire prior art as applicable as to the limitations of the claims. It is respectfully requested from the applicant, in preparing the response, to consider fully the entire references as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior arts or disclosed by the examiner.

Conclusion

Prior arts made of record, not relied upon:

US patent 7,003,674to Hamlin

US 2001/00423043 to SHEAR et al.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Taghi T. Arani whose telephone number is (571) 272-3787. The examiner can normally be reached on 8:00-5:30 Mon-Fri.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Taghi T. Arani, Ph.D.
Primary examiner
Art Unit 2131
3/14/2006